UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/783,112	02/14/2001	Josh N. Hogan	10971806-3	2220

7590 11/16/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
11/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/783,112
Filing Date: February 14, 2001
Appellant(s): HOGAN, JOSH N.

Hugh P. Gortler, Esq.
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/1/07 appealing from the Office action mailed 2/26/07.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

4377862	Koford	3-1983
4,527,273	Hibi	7-1985

For illustrative purposes, this Answer also makes reference to:

Schneier, Bruce. "Applied Cryptography, 2nd Edition" ©1996 pages 13-15

Cerf, Vint. "RFC 0020: ASCII Format for Network Interchange" ©1969 pages 1-9

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim 28 is rejected under 35 U.S.C. 102(b) as being anticipated by Koford et al. (U.S. Patent 4,377,862).

Regarding claim 28:

Koford discloses a data controller comprising a processor (col. 9, lines 1-10) for performing a bitwise XOR of an encryption mask (secret key, col. 8, lines 55-67) and a block of ECC-encoded data (col. 4, lines 35-40; col. 5, lines 43-55), a product of the bitwise XOR being an encrypted block (col. 10, lines 15-30).

Claims 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hibi et al. (U.S. Patent 4,527,723) in view of Koford.

Regarding claim 26:

Hibi discloses a computer system comprising: a computer bus (the connections of col. 4, lines 5-15; and Figure 2); a host processor programmed to perform error code correction (element 4 of Figure 2, and col. 4, lines 20-30); and a drive (col. 4, lines 5-15) providing a block of data via the computer bus to the host processor for error code correction (col. 4, lines 20-30).

Hibi does not disclose wherein the drive encrypts the ECC-encoded block with an encryption mask to produce an encrypted block, which would then be provided over the

bus to the host processor. However, Koford discloses performing a bitwise XOR of an encryption mask and a block of ECC-encoded data to produce an encrypted block (col. 8, lines 55-67; col. 10, lines 15-30) and providing the encrypted block to the computer bus to be sent to a host processor for error code correction (col. 10, lines 30-65; col. 14, lines 35-45). It would have been obvious to one of ordinary skill during at least the time the prior art disclosures were made to encrypt the data being sent between the disk drive and the CPU in the Hibi invention. The motivation for doing so would be to increase the sophistication of the error control techniques without reducing the data capacity of the communication system (Koford, col. 15, lines 25-37), in part by complying with what was at the time of the prior art a U.S. Department of Commerce encryption standard (Koford, col. 8, lines 55-60).

Regarding claim 27:

Hibi discloses a drive comprising a reader that provides blocks of ECC-encoded data (col. 4, lines 20-30). Although the ECC data is provided to a CPU by a controller over a communications channel, Hibi does not disclose wherein the controller performs a bitwise XOR encryption of said ECC-encoded data. However, as discussed above Koford discloses a controller for performing a bitwise XOR of an encryption mask and ECC-encoded data to produce an encrypted block (see the rejection of claim 27 for pertinent passages from Koford). It would have been obvious to one of ordinary skill during at least the time the prior art disclosures were made to encrypt the data being sent between the disk drive and the CPU in the Hibi invention. The motivation for doing

so would be to increase the sophistication of the error control techniques without reducing the data capacity of the communication system (Koford, col. 15, lines 25-37), in part by complying with what was at the time of the prior art a U.S. Department of Commerce encryption standard (Koford, col. 8, lines 55-60).

(10) Response to Argument

With respect to Appellant's arguments regarding claim 28, it is noted that Koford indisputably discloses a data controller comprising a processor (the module 88 of Figure 4, which in at least one embodiment of Koford is a set of instructions executed by a CPU - see col. 9, lines 26-31) performing a bitwise XOR (col. 10, lines 15-30) of an encryption mask (the secret key, comprised of "encipher/decipher characters": Ibid) and a block of data (the "plaintext" tier 1 packet data, "plaintext" being an art-specific term for unencrypted data: Koford, Ibid), a product of the bitwise XOR being an encrypted block (the "ciphertext" tier 1 packet data, "ciphertext" being an art-specific term for encrypted data: Koford: Ibid). For the convenience of the Board, Examiner also refers to the "Applied Cryptography 2nd Edition" reference, originally entered into the record on 11/10/04, which explains in detail the particulars of XOR as an encryption algorithm; [1] in particular, it is observed that as XOR when employed as an encryption algorithm is an operation on bits (Schneier, page 13), thus its use in Koford would inherently be a "bitwise XOR" operation.

[1] It is very important to note that Schneier's discovery that XOR is an "embarrassment" and "trivial to break" is not relevant here, as Koford's invention predates Schneier by fourteen years; to the contrary, at the time of the Koford invention, XOR was recommended by the U.S. Department of Commerce National Standards Bureau as an effective encryption means (col. 8, lines 55-60; col. 10, lines 25-30).

Upon closer examination, Examiner concedes that Appellant's analysis regarding the fact that the tier 1 data is encrypted before a checksum is computer is correct; however, what Appellant has failed to consider is that the input provided to the Koford invention could plausibly conform to an ECC-encoded block of data, as Koford understood the term. Consequently, Examiner maintains that the claim's recitation of "ECC-encoding" is not a structural difference that would distinguish the claim over the prior art: *In re Schreiber*, 128 F.3d 1473, 1477-78, 44 USPQ2d 1429, 1431-32 (Fed. Cir. 1997).

Koford discloses that the tier 1 data that is provided to the encryption unit is standard ASCII code (col. 4, lines 45-50); however, prior to any other processing of the data to be transmitted the extraneous start, stop, and parity bits are removed, leaving only the pure ASCII bit sequences that comprise the characters to be transmitted (col. 4, lines 50-55). Elsewhere, Koford discloses that, for the purposes of that invention, an ECC-encoded block of data is one that has a checksum appended to it, said checksum being comprised of the remainder of modulo 2 division of all the bits in the packet by a generator polynomial (col. 5, lines 45-55). In the preferred embodiment of Koford, the polynomial is $X^{16} + X^{12} + X^5 + 1$ (col. 5, lines 55-60), which corresponds to the binary numeral `10001000000100001`.

As one example to demonstrate that an overlap exists, consider the following ASCII string: `GYORFI` As is extremely well known in the art, each 7-bit ASCII character can be alternately expressed as a binary value, and vice versa (see the enclosed RFC

0020 reference for more information). Thus the binary values for each of the characters in that string are:

G = 1000111 Y = 1011001 O = 1001111

R = 1010010 F = 1000110 I = 1001001

Correspondingly, the string formed from each of those characters would be the concatenation of each of those values, written as:

1000111101100110011111010010100011010010 01

Dividing this number modulo 2 by the generator polynomial disclosed by Koford yields the result 01000101001111. Once again referring to the ASCII chart, this binary value is equivalent to the ASCII string comprised of the quotation mark character (0100010) and the capital letter O (1001111). Clearly, even a checksum for the error corrected code method employed by Koford can be expressed as an ASCII string. So if the Koford invention were presented with the ASCII string GYORFI"O this string would itself be an ECC-encoded block of data, just as Koford defines the term. It is further observed that Koford places no limitations as to particular sequences of ASCII characters that can be provided as input to that invention; furthermore, although it suggests a preferred packet size of 40 data characters (col. 4, lines 62-66), this is not a mandatory restriction as to the size of the data to be transmitted, and there is no disclosure in Koford of any lower or upper limit as to the number of characters that can be transmitted in a packet, regardless of tier.

In short, Appellant's argument fails to establish that the encryption of "ECC-encoded" data is a structural difference over the prior art. By way of analogy, claim 28

is the equivalent of claiming in the present day and age an automobile as a general invention, and subsequently arguing that the claimed automobile differs over the prior art in that the chassis of said claimed automobile is painted blue. Just as a vehicle will function regardless of its particular color, so too will the Koford invention encrypt blocks of data, whether or not the data to be encrypted conforms to some form of ECC-encoding. And as has been established above, there exist strings of ASCII characters that conform to Koford's definition of an ECC-encoded block of data.

It is additionally observed that the various aspects of the instant invention that Appellant alleges are not disclosed by the Koford reference (e.g., that Koford fails to teach that XOR encryption preserves ECC integrity, or whether or not Koford leaves blocks vulnerable to theft and unauthorized copying - see the Appeal Brief, page 6, the last three paragraphs), are not recited in the claims being rejected. Although claims are read in light of the specification, limitations from the specification are not read into the claims: *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In this case, claim 28 merely recites that the end result of the XOR encryption is an "encrypted block". There is absolutely no requirement that the encrypted block have any other special properties such as those that Appellant alleges to have discovered in the Appeal Brief. Claim 28 even fails to stipulate that ECC encoded blocks are sent over a computer bus, let alone doing so in a secure fashion. The claim is simply directed to the overbroad concept of an apparatus using XOR to perform encryption on a block of data, which Examiner maintains had long been anticipated by Koford.

Appellant's arguments regarding claim 26 and 27.appear to be predicated on the assumption that Koford does not disclose the limitations these claims have in common with claim 28; therefore, Examiner asks that the rejections of these claims be upheld for substantially similar reasons as discussed above regarding claim 28.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Thomas Gyorfi

Examiner, Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

HOSUK SONG
PRIMARY EXAMINER

Kim Vu KV

Supervisory Examiner (AU 2135)

Hosuk Song HS

Primary Examiner (AU 2135)

Attachment: Network Interchange, Oct. 16, 1969

Network Working Group
Request for Comments: 20

Vint Cerf
UCLA
October 16, 1969

ASCII format for Network Interchange

For concreteness, we suggest the use of standard 7-bit ASCII embedded in an 8 bit byte whose high order bit is always 0. This leads to the standard code given on the attached page, copies from USAS X3, 4-1968. This code will be used over HOST-HOST primary connections. Break characters will be defined by the receiving remote host, e.g. SRI uses "." (ASCII X'2E' or 2/14) as the end-of-line character, where as UCLA uses X'OD' or 0/13 (carriage return).

USA Standard Code for Information Interchange

1. Scope

This coded character set is to be used for the general interchange of information among information processing systems, communication systems, and associated equipment.

2. Standard Code

B \ b7 ---------->	0	0	0	0	1	1	1	1
I \ b6 ---------->	0	0	1	1	0	0	1	1
T \ b5 -------->	0	1	0	1	0	1	0	1
S								
COLUMN->	0	1	2	3	4	5	6	7
b4 b3 b2 b1 ROW								
0 0 0 0 0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1 1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0 2	STX	DC2	"	2	B	R	b	r
0 0 1 1 3	ETX	DC3	#	3	C	S	c	s
0 1 0 0 4	EOT	DC4	$	4	D	T	d	t
0 1 0 1 5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0 6	ACK	SYN	&	6	F	V	f	v
0 1 1 1 7	BEL	ETB	'	7	G	W	g	w
1 0 0 0 8	BS	CAN	(	8	H	X	h	x
1 0 0 1 9	HT	EM	)	9	I	Y	i	y
1 0 1 0 10	LF	SUB	*	:	J	Z	j	z
1 0 1 1 11	VT	ESC	+	;	K	[	k	{
1 1 0 0 12	FF	FS	,	<	L	\	l	|
1 1 0 1 13	CR	GS	-	=	M	]	m	}
1 1 1 0 14	SO	RS	.	>	N	^	n	~
1 1 1 1 15	SI	US	/	?	O	_	o	DEL

3. Character Representation and Code Identification

The standard 7-bit character representation, with b7 the high-order bit and b1 the low-order bit, is shown below:

EXAMPLE: The bit representation for the character "K," positioned in column 4, row 11, is

```
b7 b6 b5 b4 b3 b2 b1
1  0  0  1  0  1  1
```

The code table position for the character "K" may also be represented by the notation "column 4, row 11" or alternatively as "4/11." The decimal equivalent of the binary number formed by bits b7, b6, and b5, collectively, forms the column number, and the decimal equivalent of the binary number formed by bits b4, b3, b2, and b1, collectively, forms the row number.

The standard code may be identified by the use of the notation ASCII or USASCII.

The notation ASCII (pronounced as'-key) or USASCII (pronounced you-sas'-key) should ordinarily be taken to mean the code prescribed by the latest issue of the standard. To explicitly designate a particular (perhaps prior) issue, the last two digits of the year of issue may be appended, as, "ASCII 63" or "USASCII 63".

4. Legend

4.1 Control Characters

NUL Null	DLE Data Link Escape (CC)
SOH Start of Heading (CC)	DC1 Device Control 1
STX Start of Text (CC)	DC2 Device Control 2
ETX End of Text (CC)	DC3 Device Control 3
EOT End of Transmission (CC)	DC4 Device Control 4 (Stop)
ENQ Enquiry (CC)	NAK Negative Acknowledge (CC)
ACK Acknowledge (CC)	SYN Synchronous Idle (CC)
BEL Bell (audible or attention signal)	ETB End of Transmission Block (CC)
BS Backspace (FE)	CAN Cancel
HT Horizontal Tabulation (punched card skip) (FE)	EM End of Medium
LF Line Feed (FE)	SUB Substitute
VT Vertical Tabulation (FE)	ESC Escape
FF Form Feed (FE)	FS File Separator IS)
CR Carriage Return (FE)	GS Group Separator (IS)
SO Shift Out	RS Record Separator (IS)
SI Shift In	US Unit Separator (IS)
	DEL Delete [1]

NOTE: (CC) Communication Control
(FE) Format Effector
(IS) Information Separator

[1] In the strict sense, DEL is not a control character. (See 5.2)

4.2 Graphic Characters

Column/Row	Symbol	Name
2/0	SP	Space (Normally Non-Printing)
2/1	!	Exclamation Point
2/2	"	Quotation Marks (Diaeresis [2])
2/3	#	Number Sign [3,4]
2/4	$	Dollar Sign
2/5	%	Percent
2/6	&	Ampersand
2/7	'	Apostrophe (Closing Single Quotation Mark Acute Accent [2])
2/8	(	Opening Parenthesis
2/9	)	Closing Parenthesis
2/10	*	Asterisk
2/11	+	Plus
2/12	,	Comma (Cedilla [2])
2/13	-	Hyphen (Minus)
2/14	.	Period (Decimal Point)
2/15	/	Slant
3/10	:	Colon
3/11	;	Semicolon
3/12	<	Less Than
3/13	=	Equals
3/14	>	Greater Than
3/15	?	Question Mark
4/0	@	Commercial At [3]
5/11	[	Opening Bracket [3]
5/12	\	Reverse Slant [3]
5/13	]	Closing Bracket [3]
5/14	^	Circumflex [2,3]
5/15	_	Underline
6/0	`	Grave Accent [2,3] (Opening Single Quotation Mark)
7/11	{	Opening Brace [3]
7/12	|	Vertical Line [3]
7/13	}	Closing Brace [3]
7/14	~	Overline [3] (Tilde [2]; General Accent [2])

2 The use of the symbols in 2/2, 2/7, 2/12, 5/14, /6/0, and 7/14 as diacritical marks is described in Appendix A, A5.2

3 These characters should not be used in international interchange without determining that there is agreement between sender and recipient. (See Appendix B4.)

4 In applications where there is no requirement for the symbol #, the symbol (Pounds Sterling) may be used in position 2/3.

5. Definitions

5.1 General

(CC) Communication Control: A functional character intended to control or facilitate transmission of information over communication networks.

(FE) Format Effector: A functional character which controls the layout or positioning of information in printing or display devices.

(IS) Information Separator: A character which is used to separate and qualify information in a logical sense. There is a group of four such characters, which are to be used in a hierarchical order.

5.2 Control Characters

NUL (Null): The all-zeros character which may serve to accomplish time fill and media fill.

SOH (Start of Heading): A communication control character used at the beginning of a sequence of characters which constitute a machine-sensible address or routing information. Such a sequence is referred to as the "heading." An STX character has the effect of terminating a heading.

STX (Start of Text): A communication control character which precedes a sequence of characters that is to be treated as an entity and entirely transmitted through to the ultimate destination. Such a sequence is referred to as "text." STX may be used to terminate a sequence of characters started by SOH.

ETX (End of Text): A communication control character used to terminate a sequence of characters started with STX and transmitted as an entity.

EOT (End of Transmission): A communication control character used to indicate the conclusion of a transmission, which may have contained one or more texts and any associated headings.

ENQ (Enquiry): A communication control character used in data communication systems as a request for a response from a remote station. It may be used as a "Who Are You" (WRU) to obtain identification, or may be used to obtain station status, or both.

ACK (Acknowledge): A communication control character transmitted by a receiver as an affirmative response to a sender.

BEL (Bell): A character for use when there is a need to call for human attention. It may control alarm or attention devices.

BS (Backspace): A format effector which controls the movement of the printing position one printing space backward on the same printing line. (Applicable also to display devices.)

HT (Horizontal Tabulation): A format effector which controls the movement of the printing position to the next in a series of predetermined positions along the printing line. (Applicable also to display devices and the skip function on punched cards.)

LF (Line Feed): A format effector which controls the movement of the printing position to the next printing line. (Applicable also to display devices.) Where appropriate, this character may have the meaning "New Line" (NL), a format effector which controls the movement of the printing point to the first printing position on the next printing line. Use of this convention requires agreement between sender and recipient of data.

VT (Vertical Tabulation): A format effector which controls the movement of the printing position to the next in a series of predetermined printing lines. (Applicable also to display devices.)

FF (Form Feed): A format effector which controls the movement of the printing position to the first pre-determined printing line on the next form or page. (Applicable also to display devices.)

CR (Carriage Return): A format effector which controls the movement of the printing position to the first printing position on the same printing line. (Applicable also to display devices.)

SO (Shift Out): A control character indicating that the code combinations which follow shall be interpreted as outside of the character set of the standard code table until a Shift In character is reached.

SI (Shift In): A control character indicating that the code combinations which follow shall be interpreted according to the standard code table.

DLE (Data Link Escape): A communication control character which will change the meaning of a limited number of contiguously following characters. It is used exclusively to provide supplementary controls in data communication networks.

DC1, DC2, DC3, DC4 (Device Controls): Characters for the control of ancillary devices associated with data processing or telecommunication systems, more especially switching devices "on" or "off." (If a single "stop" control is required to interrupt or turn off ancillary devices, DC4 is the preferred assignment.)

NAK (Negative Acknowledge): A communication control character transmitted by a receiver as a negative response to the sender.

SYN (Synchronous Idle): A communication control character used by a synchronous transmission system in the absence of any other character to provide a signal from which synchronism may be achieved or retained.

ETB (End of Transmission Block): A communication control character used to indicate the end of a block of data for communication purposes. ETB is used for blocking data where the block structure is not necessarily related to the processing format.

CAN (Cancel): A control character used to indicate that the data with which it is sent is in error or is to be disregarded.

EM (End of Medium): A control character associated with the sent data which may be used to identify the physical end of the medium, or the end of the used, or wanted, portion of information recorded on a medium.

(The position of this character does not necessarily correspond to the physical end of the medium.)

SUB (Substitute): A character that may be substituted for a character which is determined to be invalid or in error.

ESC (Escape): A control character intended to provide code extension (supplementary characters) in general information interchange. The Escape character itself is a prefix affecting the interpretation of a limited number of contiguously following characters.

FS (File Separator), GS (Group Separator), RS (Record Separator), and US (Unit Separator): These information separators may be used within data in optional fashion, except that their hierarchical relationship shall be: FS is the most inclusive, then GS, then RS, and US is least inclusive. (The content and length of a File, Group, Record, or Unit are not specified.)

DEL (Delete): This character is used primarily to "erase" or "obliterate" erroneous or unwanted characters in perforated tape. (In the strict sense, DEL is not a control character.)

5.3 Graphic Characters

SP (Space): A normally non-printing graphic character used to separate words. It is also a format effector which controls the movement of the printing position, one printing position forward. (Applicable also to display devices.)

6. General Considerations

6.1 This standard does not define the means by which the coded set is to be recorded in any physical medium, nor does it include any redundancy or define techniques for error control. Further, this standard does not define data communication character structure, data communication formats, code extension techniques, or graphic representation of control characters.

6.2 Deviations from the standard may create serious difficulties in information interchange and should be used only with full cognizance of the parties involved.

6.3 The relative sequence of any two characters, when used as a basis for collation, is defined by their binary values.

6.4 No specific meaning is prescribed for any of the graphics in the code table except that which is understood by the users. Furthermore, this standard does not specify a type style for the printing or display of the various graphic characters. In specific applications, it may be desirable to employ distinctive styling of individual graphics to facilitate their use for specific purposes as, for example, to stylize the graphics in code positions 2/1 and 5/15 into those frequently associated with logical OR (|) and logical NOT (252), respectively.

6.5 The appendixes to this standard contain additional information on the design and use of this code.

[This RFC was put into machine readable form for entry]
[into the online RFC archives by Robbie Bennet 9/99]